Department of the Interior
Infrastructure Services Division

Standard Operating Procedure

Web Filter Exception Request Process

April 24, 2012

Table of Contents

1. Purpose

The purpose of this document is to provide a step by step description of the new web filter exception request process. This new process will address the shortcomings of the paper based exception process currently in practice. Once fully implemented, the new process will utilize a form within the Remedy ticketing system to automate the request process.

1.1 Change History

The following Change History Log contains a record of changes made to this **section**.

Date Published/ Revised	Version No.	Author	Section/Description of Change
Nov 28, 2011	1.0	Chris Brooks	▪ Initial Draft
Dec 21, 2011	1.1	Andrew Hogarth	▪ Updated Draft, revising Classify to Category
Jan 3, 2012	1.2	Andrew Hogarth	▪ Made minor edits based on feedback from ITST members. ▪ Updated Remedy URL ▪ Changed document from Draft to Final.
Apr 24, 2012	1.3	Andrew Hogarth	▪ Added steps and screen shots for the newly added Scope specification process (Section 1.5, New Process, beginning with step 8) and Appendix A

1.2 Approvals

The following table contains a list of reviewers and approvals for this document.

Date Reviewed	Approval/Disapproval	Reviewed by (Name, Title)
		Robert Lewis
		Quentin Cheuk

1.3 Scope

The procedures outlined herein are applicable to the process of requesting a change to the Blue Coat web filtering policies. The filtering policies in the Blue Coat proxies are configured in accordance with applicable DOI policies that define the acceptable use of the Internet. This procedure does not invalidate the requirement for opening a CRQ (change request) with the appropriate CCB (Change Control Board) for any additional Internet traffic required in support of a project.

1.4 Points of Contact

Name	Function	Phone	Email
Chris Brooks	Information Assurance Engineer	703-648-5532	Christopher_Brooks@ios.doi.gov
Andrew Hogarth	Information Assurance Engineer	703-648-5673	Andrew_Hogarth@ios.doi.gov
Tony Barros	Information Assurance Engineer	703-648-5564	Jose_Barros@ios.doi.gov

1.5 Web Filter Exception Request Process

The current web filter exception request process works in the follow manner:

1. User receives block page while attempting to access a website via browser.
2. User accesses the “Submit an Unblock Request Form” link from the block page where they are served the Web Filter Exception Request Form (WFER) in Microsoft Word.
3. User completes the relevant sections of the form and submits form to his manager for signature.
4. The manager will print the form, sign it and scan the form in so it can be submitted to either the Bureau Security representative or the Bureau Chief Information Security Officer for approval and action.
5. The BCISO or Security representative will print, sign, and scan document in again. The bureau approved form is then forwarded to Web_Filtering@ios.doi.gov for action.
6. The Web Filtering Team then checks the form for accuracy and if correct, forwards the email to management for approval.
7. If approved, the form is returned to the Web Filtering Team and the Blue Coat proxies are changed so access is established to the requested website.
8. Email returned to BCISO verifying change to proxies to permit the requested access.

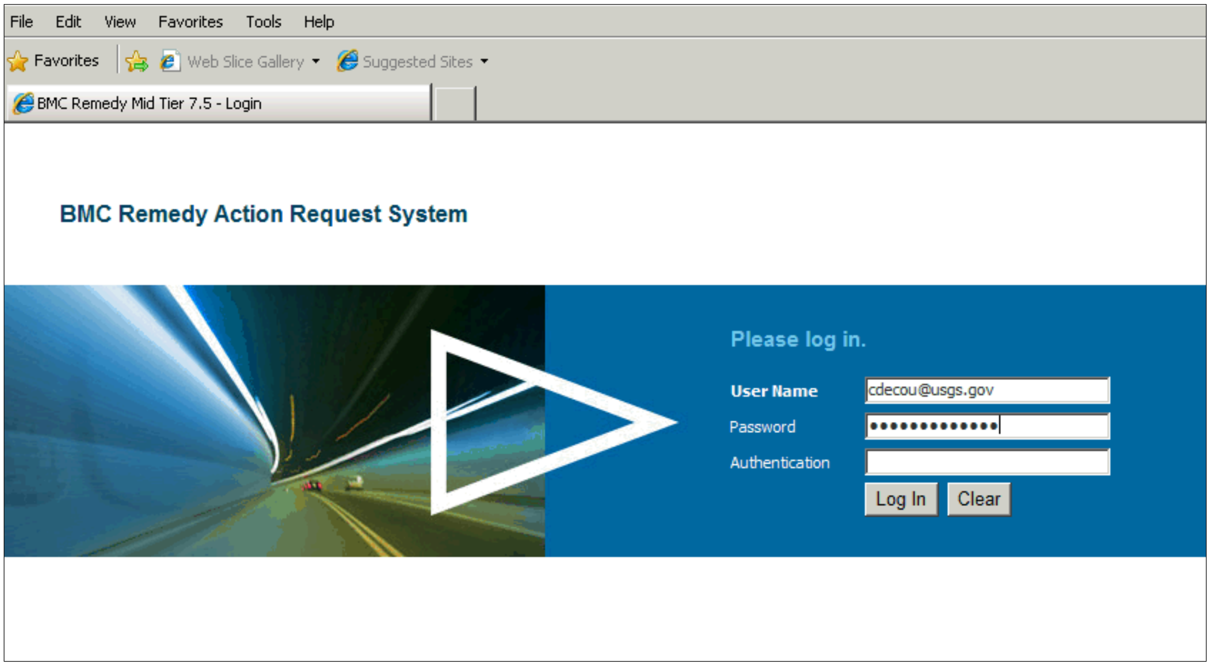
The new web filter exception request process will improve on the current process by employing a form in the Remedy ticketing system that will replace the old paper form. This will also enable the form to be digitally signed/approved by the user’s manager, Bureau CISO/Security Team Representative, and management at DOI. These improvements should not only increase the efficiency in the manner the WFERs are processed but allow for improved tracking of active and completed requests.

The new web filter exception request will work as follows:

1. User receives block page while attempting to access a website via browser.
2. User accesses the “Submit an Unblock Request Form” link from the block page where they will be redirected to the Remedy ticketing system at the following link:

   https://support.usgs.gov/arsys/forms/igskahcigssd02.gs.doi.net/DOI%3AWeb+Access+Exception+Request/?mode=CREATE

   If prompted for a login, the user will enter into the “User Name” field their User Principal Name (UPN), which is their Active Directory **User ID** and domain name separated by an @ symbol (e.g., userid@ios.doi.gov, userid@blm.gov), and into the “Password” field they will enter their domain logon password. The “Authentication” field can be ignored. Please note that in some cases the user’s UPN will be the same as their email address, but this is not always the case (e.g., UPN: userid@ios.doi.gov; Email: user_id@ios.doi.gov). If the user has trouble getting logged in, they can call the USGS Service Desk at 1-866-447-4375. Additional support access options are available at the following link http://support.usgs.gov.


File Edit View Favorites Tools Help
Favorites
Web Slice Gallery
Suggested Sites
BMC Remedy Mid Tier 7.5 - Login
Log In
Clear

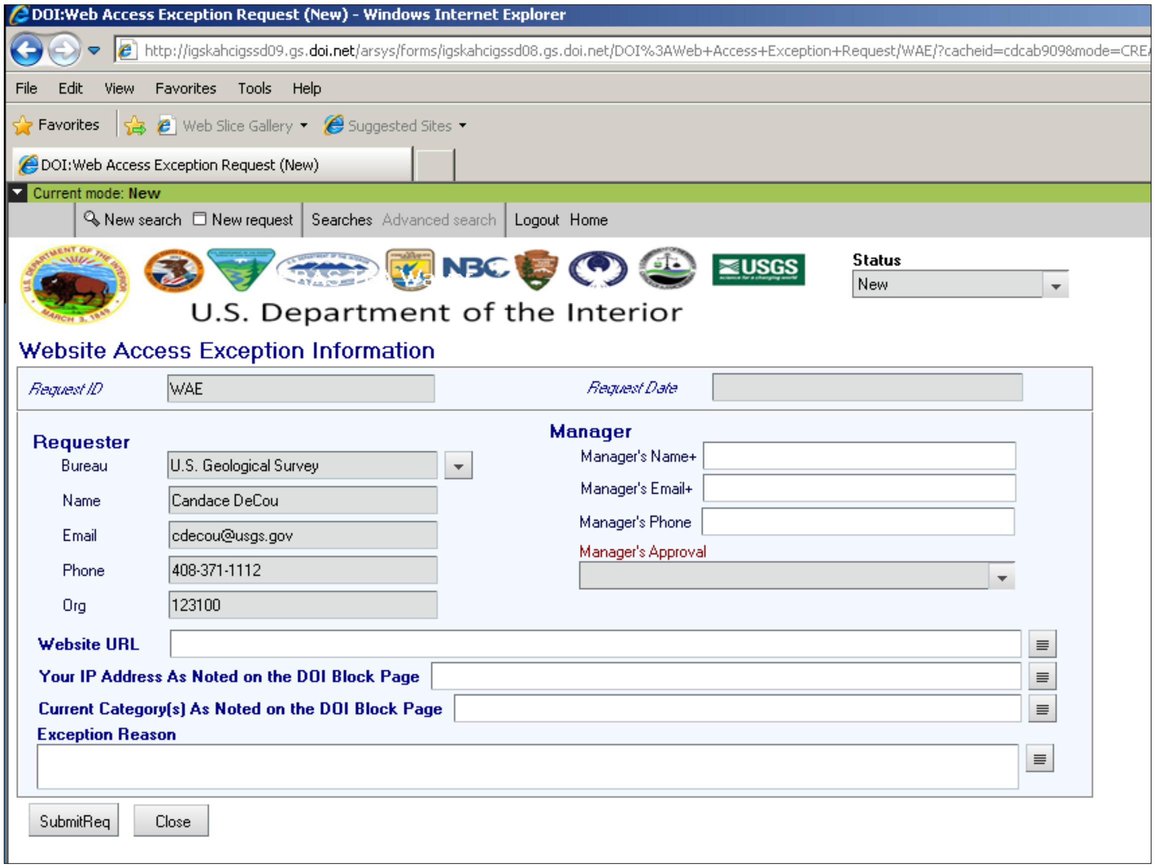
BMC Remedy Action Request System

Please log in.

User Name	cdecou@usgs.gov
Password	•••••••••••••
Authentication	

Figure 1 - Login Prompt for Remedy

3. After logging in or following the URL noted above, the user will enter the Web Access Exception Request form in New mode. The Requester information area will auto-populate with the user's information as it exists in the system.


DOI:Web Access Exception Request (New) - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
Web Slice Gallery
Suggested Sites
DOI:Web Access Exception Request (New)
New search
New request
Searches
Advanced search
Logout
Home
U.S. Department of the Interior
USGS
SubmitReq
Close

http://igskahcigssd09.gs.doi.net/arsys/forms/igskahcigssd08.gs.doi.net/DOI%3AWeb+Access+Exception+Request/WAE/?cacheid=cdcab909&mode=CRE

Current mode: New

Status	New

Website Access Exception Information

Request ID	WAE	Request Date	

Requester

Bureau	U.S. Geological Survey
Name	Candace DeCou
Email	cdecou@usgs.gov
Phone	408-371-1112
Org	123100

Manager

Manager's Name+	
Manager's Email+	
Manager's Phone	
Manager's Approval	

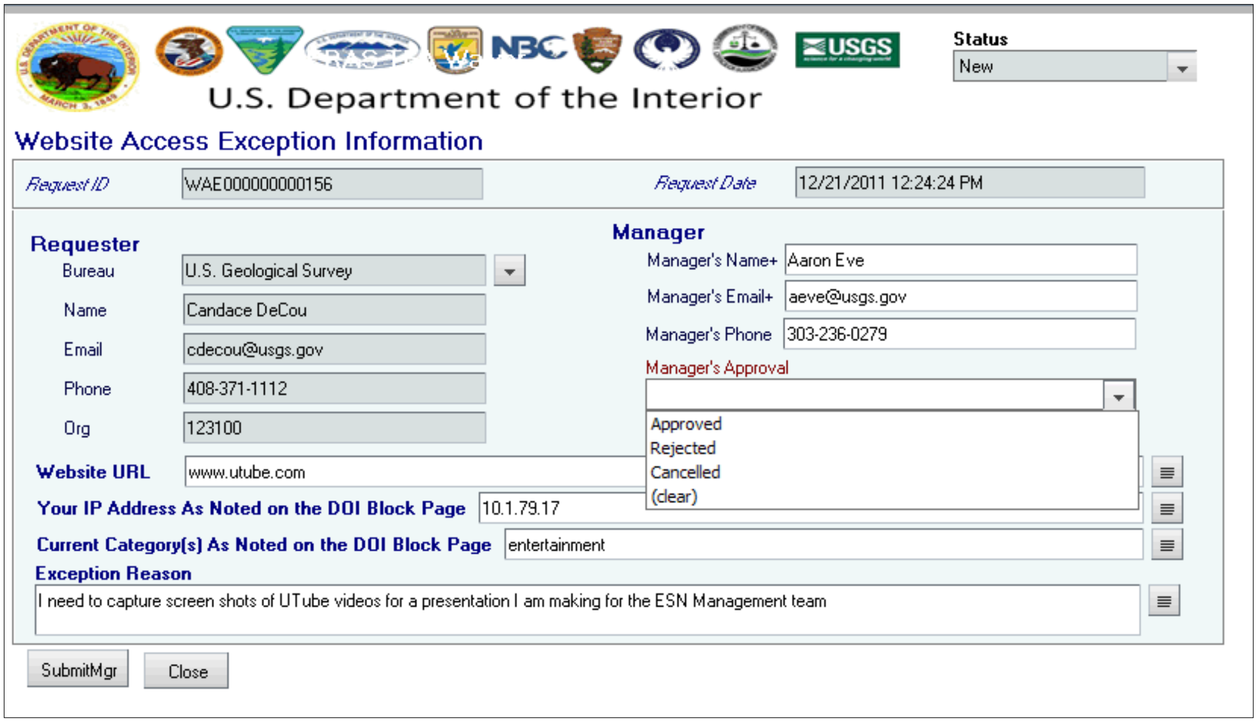
Website URL	
Your IP Address As Noted on the DOI Block Page	
Current Category(s) As Noted on the DOI Block Page	
Exception Reason	

Figure 2 - Auto-population of User Information

4. The User will also complete the Manager's Name, Website URL, their IP Address (as presented on the DOI Block Page), the Current Category(s) of the site (also copied from the block page), and Exception Reason fields; these are required entries. Once completed, the User will select the SubmitReq button which will forward the form to the user's manager for approval.

5. The manager noted in the Web Access Exception Information form will receive an email notification letting them know that the request is pending their approval. The manager can either reply to the email to have the request Approved, Rejected or Cancelled or, if they have a Remedy account, they can click on the URL link within the notification email. When replying by email, the **EXACT** word: **Approved**, **Rejected**, or **Cancelled**, must be **added** to the **beginning of the subject line**.

6. If the manager has a Remedy account and clicks on the URL link they should be automatically logged into the Remedy system to see the submitted request, from which they can make the appropriate selection from the Manager's Approval menu (Approved, Rejected, or Cancelled). After making the appropriate selection, the manager will click on the SubmitMgr button to submit the request and move it forward for Bureau CISO approval. The requester will receive an email notification with the results of the manager's approval selection.



U.S. Department of the Interior

Website Access Exception Information

Status: New

Request ID: WAE000000000156

Request Date: 12/21/2011 12:24:24 PM

Requester

Bureau: U.S. Geological Survey

Name: Candace DeCou

Email: cdecou@usgs.gov

Phone: 408-371-1112

Org: 123100

Manager

Manager's Name+: Aaron Eve

Manager's Email+: aeve@usgs.gov

Manager's Phone: 303-236-0279

Manager's Approval:

Website URL: www.utube.com

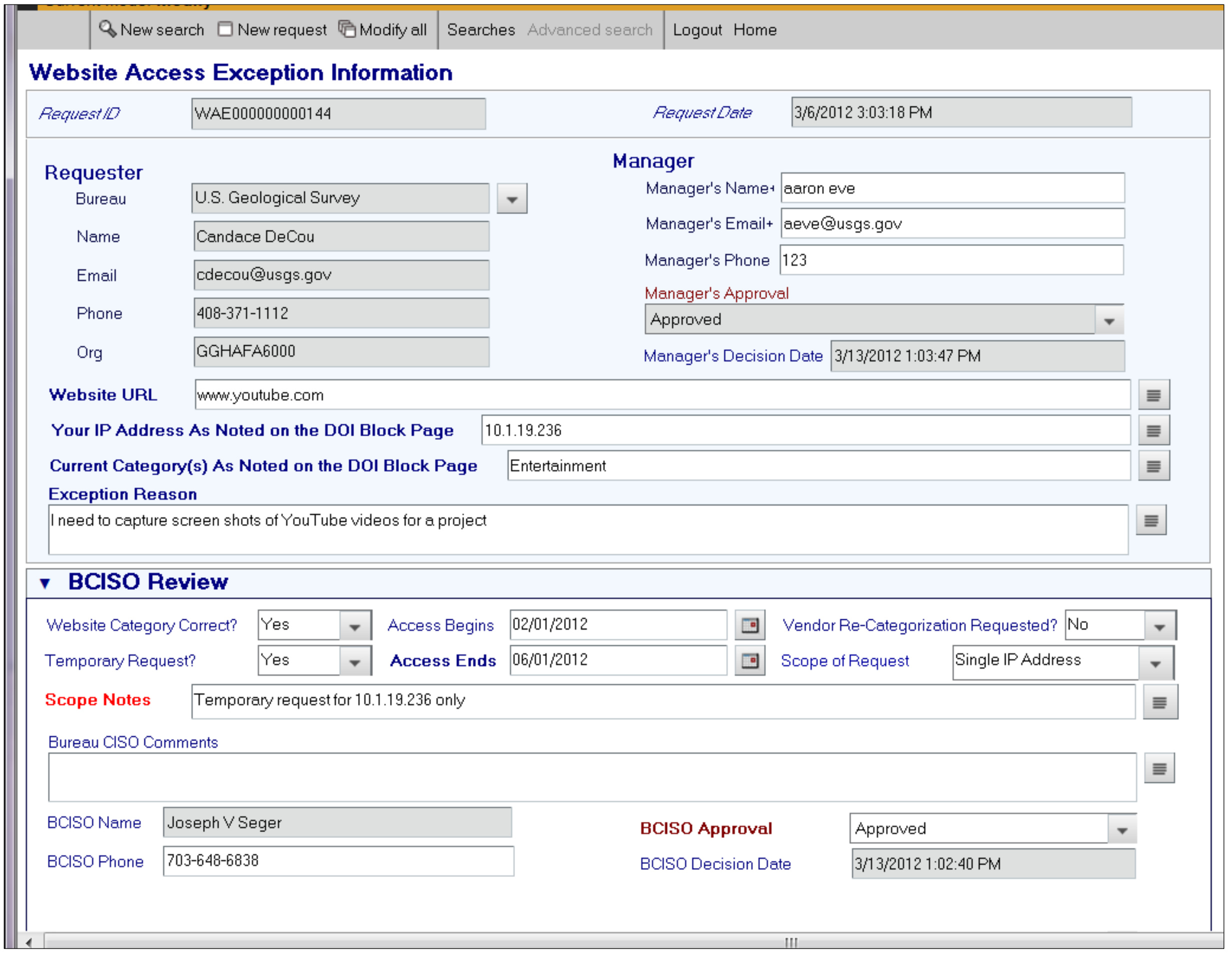
Your IP Address As Noted on the DOI Block Page: 10.1.79.17

Current Category(s) As Noted on the DOI Block Page: entertainment

Exception Reason: I need to capture screen shots of UTube videos for a presentation I am making for the ESN Management team

Figure 3 - Manager Approval Action on WFER

7. The affected bureau's primary CISO will be sent an email notification upon the manager's approval of a Web Access Exception Request. All CISO's are Remedy users and should access the system by following the link embedded in the email notification. (Note: Unlike the manager, the BCISO must use Remedy to either Approve, Reject, or Cancel the request, they can not reply to the email notification.) The BCISO Review area will be visible once the CISO accesses the form.



Website Access Exception Information

Request ID: WAE000000000144
Request Date: 3/6/2012 3:03:18 PM

Requester

Bureau	U.S. Geological Survey
Name	Candace DeCou
Email	cdecou@usgs.gov
Phone	408-371-1112
Org	GGHAFA6000

Manager

Manager's Name+	aaron eve
Manager's Email+	aeve@usgs.gov
Manager's Phone	123
Manager's Approval	Approved
Manager's Decision Date	3/13/2012 1:03:47 PM

Website URL: www.youtube.com

Your IP Address As Noted on the DOI Block Page: 10.1.19.236

Current Category(s) As Noted on the DOI Block Page: Entertainment

Exception Reason: I need to capture screen shots of YouTube videos for a project

BCISO Review

Website Category Correct?	Yes	Access Begins	02/01/2012	Vendor Re-Categorization Requested?	No
Temporary Request?	Yes	Access Ends	06/01/2012	Scope of Request	Single IP Address

Scope Notes: Temporary request for 10.1.19.236 only

Bureau CISO Comments:

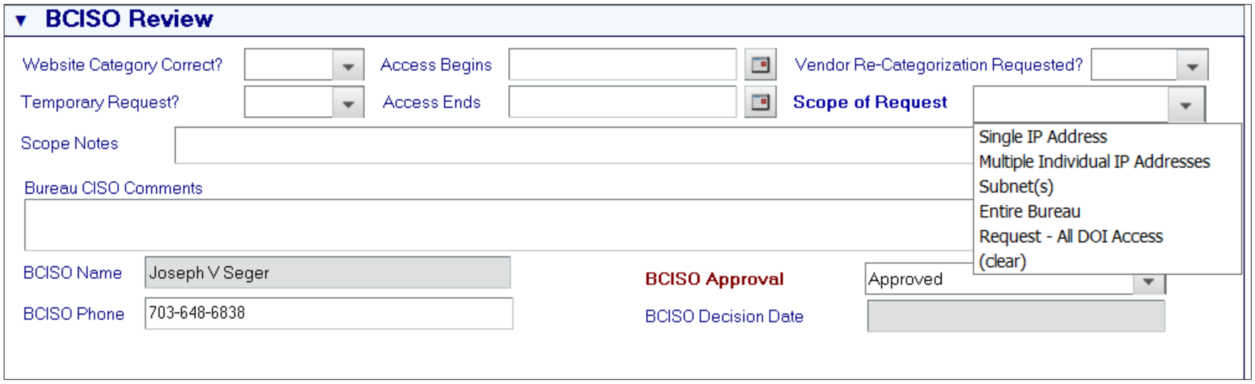
BCISO Name	Joseph V Seger	BCISO Approval	Approved
BCISO Phone	703-648-6838	BCISO Decision Date	3/13/2012 1:02:40 PM

Figure 4 - BCISO Review of WFER

8. If the Bureau CISO is approving this request, they must select one of five choices from the Scope of Request drop-down list (see Figure 5 - Scope of Request). The choices are:

Single IP Address	Specifies that the request is being approved for a single Internet routable static IP Address
Multiple Individual IP Addresses	Specifies that the request is being approved for several Internet routable static IP addresses (not a subnet)
Subnet(s)	Specifies that the request is being approved for one or more Internet routable subnets
Entire Bureau	Specifies that the request is being approved for the entire Bureau
Request - All DOI Access	Specifies that the request is being requested for access by all of DOI, and also denotes that the request is approved for the entire Bureau

Note: All IP Addresses MUST be **static** and Internet routable.



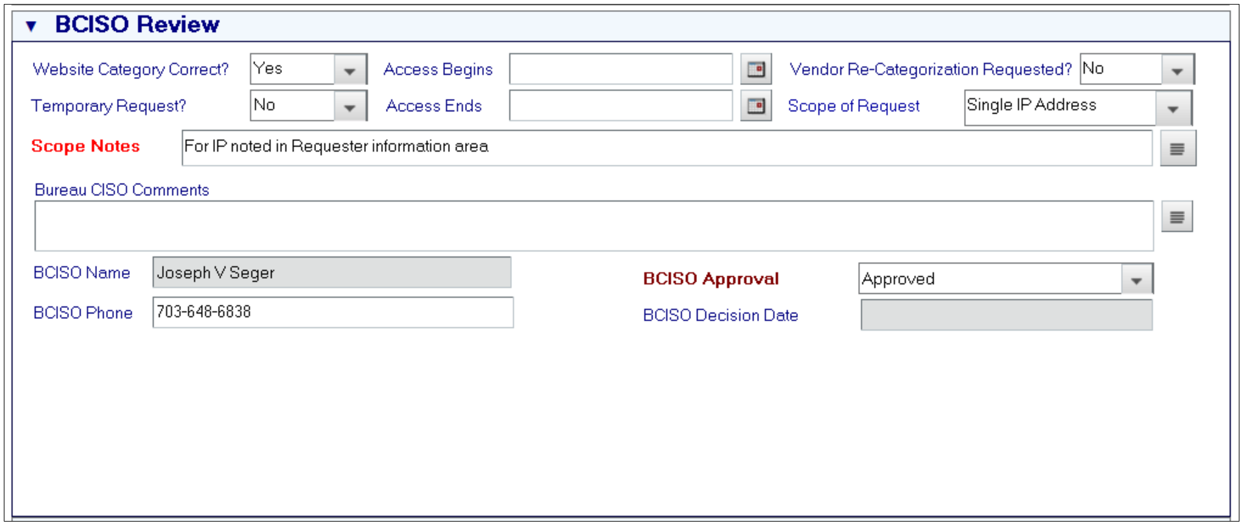
BCISO Review

Website Category Correct?
Access Begins
Vendor Re-Categorization Requested?
Temporary Request?
Access Ends
Scope of Request
Scope Notes
Bureau CISO Comments
BCISO Name: Joseph V Seger
BCISO Phone: 703-648-6838
BCISO Approval: Approved
BCISO Decision Date

Figure 5 - Scope of Request

9. A selection-specific instructional dialog box will be displayed when any of the Scope of Request choices are made. The dialog boxes provide the Bureau CISO with specific instructions on what to include in the Scope Notes field; the Scope Notes field is used to specify Internet routable static IP addresses, or Internet routable subnets and subnet masks. Screenshots of the various instructional dialog boxes are included as Appendix A.

10. Bureau CISO will select Submit button to move the request forward for the DOI management review.

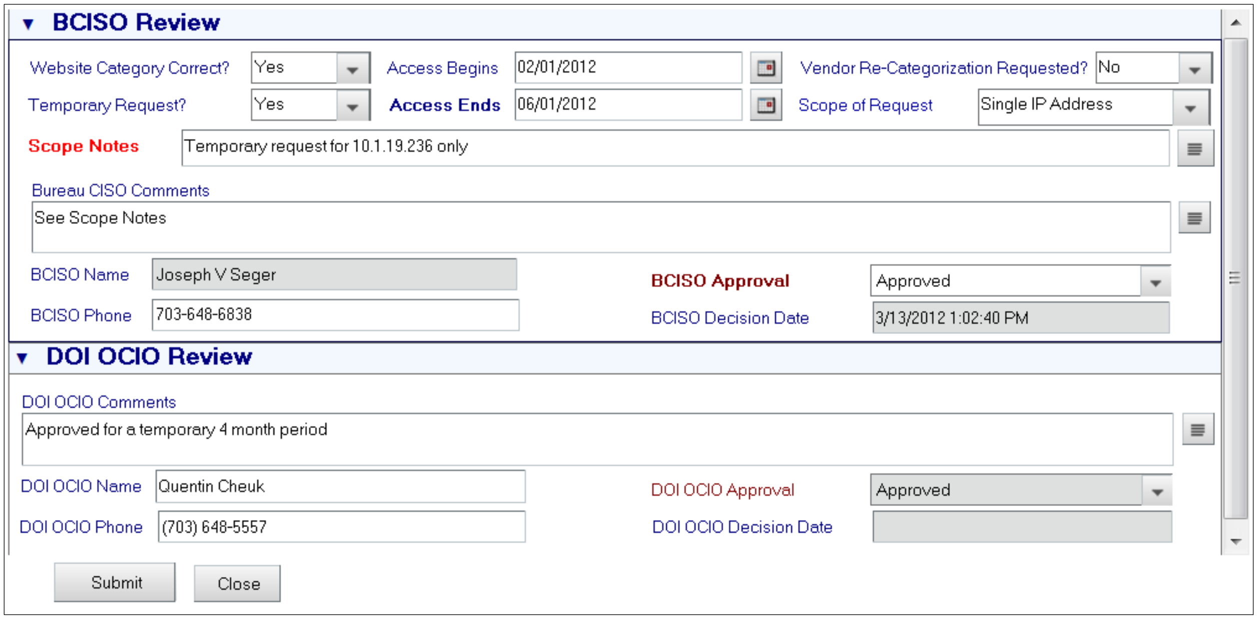


BCISO Review

Website Category Correct?: Yes
Access Begins
Vendor Re-Categorization Requested?: No
Temporary Request?: No
Access Ends
Scope of Request: Single IP Address
Scope Notes: For IP noted in Requester information area
Bureau CISO Comments
BCISO Name: Joseph V Seger
BCISO Phone: 703-648-6838
BCISO Approval: Approved
BCISO Decision Date

Figure 6 - BCISO Approval Action

11. On Approval of the request by the Bureau CISO, DOI OCIO Management will be notified of the request pending review. Once OCIO Management selects an Approval state, all parties to the request will be notified by email of the approval status.



▼ BCISO Review

Website Category Correct?	Yes	Access Begins	02/01/2012	Vendor Re-Categorization Requested?	No
Temporary Request?	Yes	Access Ends	06/01/2012	Scope of Request	Single IP Address

Scope Notes: Temporary request for 10.1.19.236 only

Bureau CISO Comments: See Scope Notes

BCISO Name	Joseph V Seger	BCISO Approval	Approved
BCISO Phone	703-648-6838	BCISO Decision Date	3/13/2012 1:02:40 PM

▼ DOI OCIO Review

DOI OCIO Comments: Approved for a temporary 4 month period

DOI OCIO Name	Quentin Cheuk	DOI OCIO Approval	Approved
DOI OCIO Phone	(703) 648-5557	DOI OCIO Decision Date	

Figure 7 - DOI OCIO Management Review/Approval

In addition, the submission of the DOI OCIO Management Approval will send an email notification to the Web Filtering team, letting them know the request is ready to be processed. Once the Web Filtering team has completed their work, they will set the Status of the request to Implemented and this will submit another email notification to the Requester that the request is now in place.

1.6 Implementation

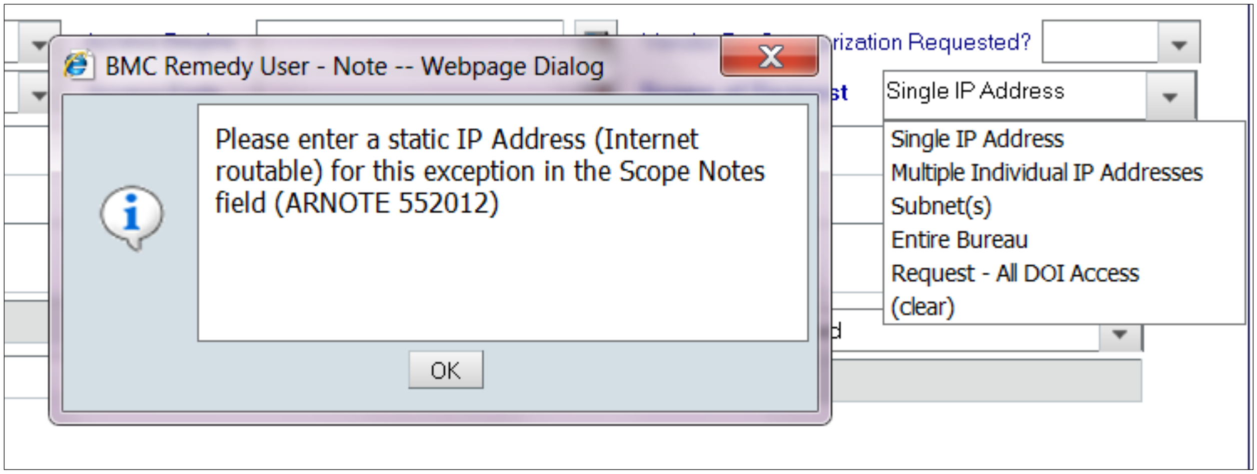
The new web filtering exception request process will not be implemented until all of the Bureau personnel involved in the approval portions of the process are notified and access to Remedy from all affected bureaus is verified. Also, minor adjustments will be completed to the standard DOI Block Page to permit the redirect from the block page to the Remedy ticketing system.

1.6.1 Troubleshooting

Troubleshooting and validation will be completed with all Bureau Security Personnel prior to the implementation of the new web filter process in the production environment. After this process is in its production state, all errors, questions, and comments can be directed to the Web Filtering Team at Web_Filtering@ios.doi.gov.

Appendix A Screenshots of Instructional Dialog boxes

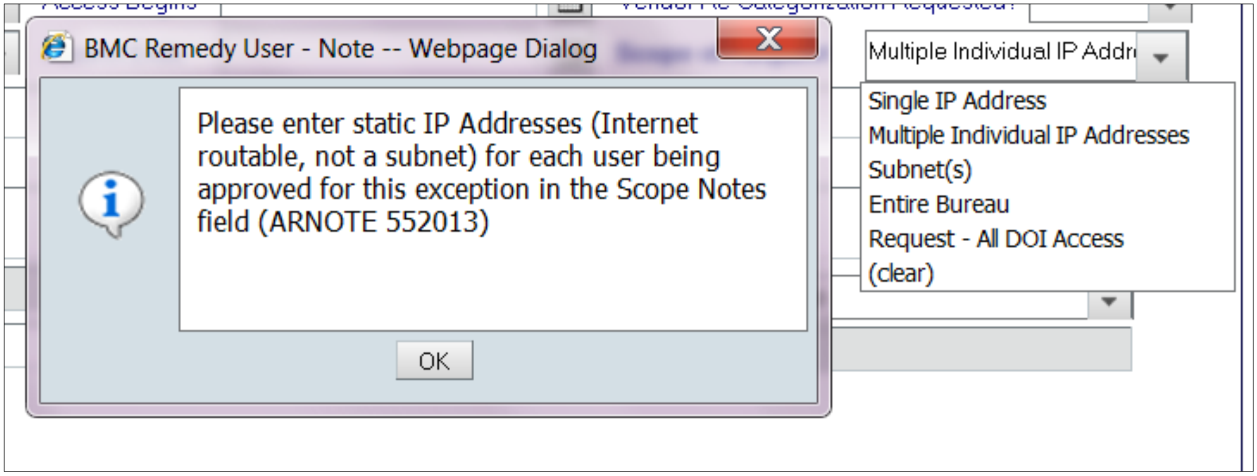
Dialog Box – Single IP Address Selection



BMC Remedy User - Note -- Webpage Dialog

Please enter a static IP Address (Internet routable) for this exception in the Scope Notes field (ARNOTE 552012)

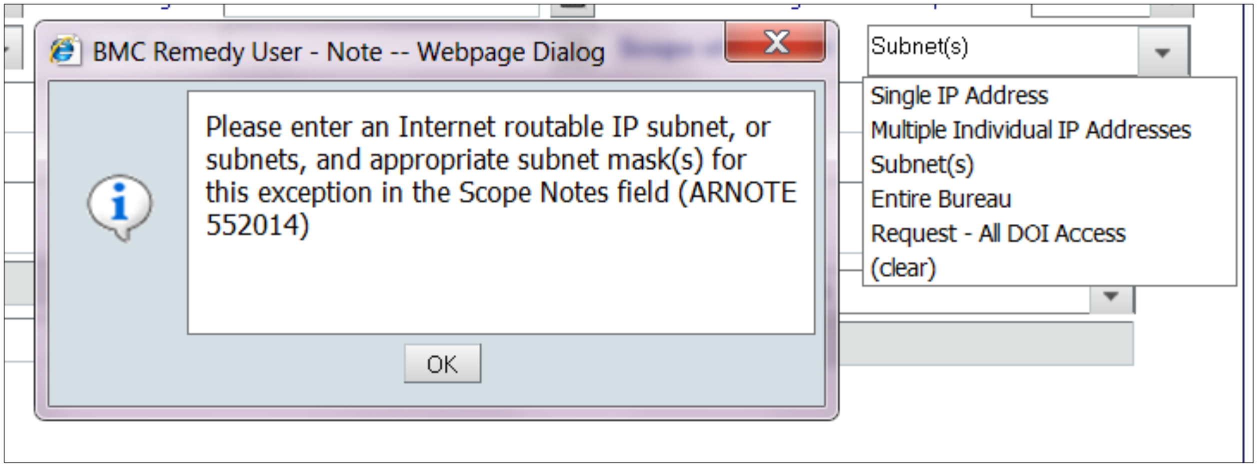
Dialog Box – Multiple Individual IP Addresses Selection



BMC Remedy User - Note -- Webpage Dialog

Please enter static IP Addresses (Internet routable, not a subnet) for each user being approved for this exception in the Scope Notes field (ARNOTE 552013)

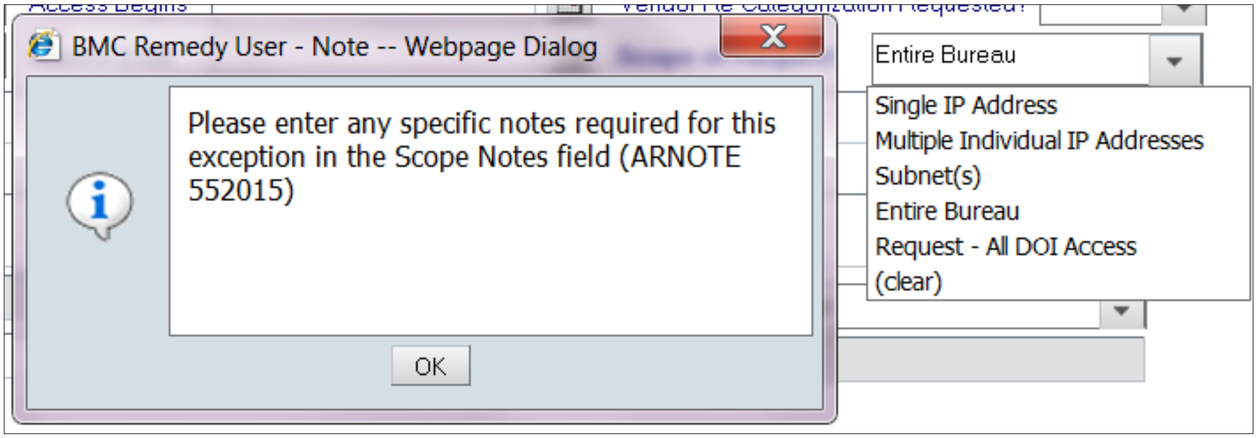
Dialog Box – Subnet(s) Selection



BMC Remedy User - Note -- Webpage Dialog

Please enter an Internet routable IP subnet, or subnets, and appropriate subnet mask(s) for this exception in the Scope Notes field (ARNOTE 552014)

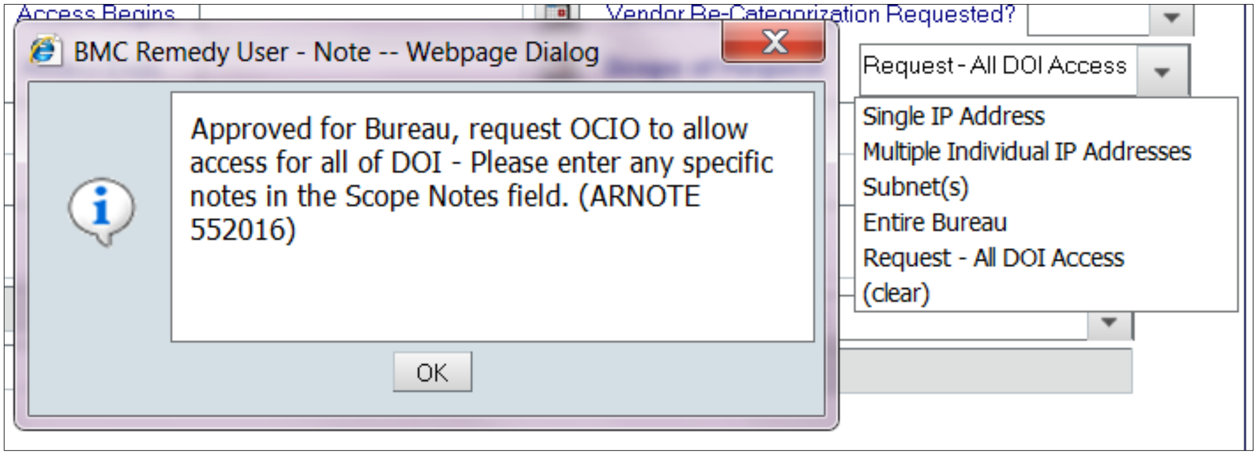
Dialog Box – Entire Bureau Selection



BMC Remedy User - Note -- Webpage Dialog

Please enter any specific notes required for this exception in the Scope Notes field (ARNOTE 552015)

Dialog Box – Request DOI Access Selection



BMC Remedy User - Note -- Webpage Dialog

Approved for Bureau, request OCIO to allow access for all of DOI - Please enter any specific notes in the Scope Notes field. (ARNOTE 552016)